An Ontological Approach to Secure MANET Management

Mark E. Orwat, Timothy E. Levin, and Cynthia E. Irvine

Computer Science Department
Naval Postgraduate School
Monterey, CA 93943
{morwat, televin, irvine}@nps.edu

Abstract

Mobile Ad hoc Networks (MANETs) rely on dynamic configuration decisions to efficiently operate in a rapidly changing environment of limited resources. The ability of a MANET to make decisions that accurately reflect the real environment depends on the quality of the input to those decisions. However, collecting and processing of the multitudinous factors related to the operation of a MANET is a significant challenge. Equally significant in current approaches to dynamic MANET management is the lack of consideration given to security factors. We show how our ontology of MANET attributes including device security and performance characteristics can be leveraged to efficiently and effectively make dynamic configuration decisions for managing a MANET.

1. Introduction

A mobile ad hoc network (MANET) is a collection of mobile, autonomous, wireless devices that form a communications network without the assistance of a fixed infrastructure. The ultimate goal of MANET network designers is to provide a self-protecting, "dynamic, self-forming, and self-healing network" for nodes on the move [1]. To maintain persistent communication and connectivity, the devices must make collective decisions regarding physical and logical configuration of the network, routing procedures, the distribution of functionality within the devices, and the network security posture. As the context of the network changes and the devices consume resources, these same decisions must periodically be revisited to ensure that the goals of the network continue to be met.

The ability of the network to meet its goals depends directly upon the input fed into the decision process. A big challenge facing MANET researchers is how to generate and capture the factors relevant to the everyday operation of the network. Equally significant in today's MANET decision algorithms is the lack of consideration given to security factors in the decisions that drive the network's organization and operation. However, the incorporation of security factors must be supported by an organizing structure that facilitates automated decision processes.

The *MANET Distributed Functions Ontology (MDFO)* described here is used to structure MANET performance and security information. An associated "operational vision" for its integration into MANET operations is presented. This ontology enhances the MANET decision processes in three ways: it gives us the ability to normalize parameters into common terms, it allows us to make inferences should values be unavailable or inconsistent, and it provides a canonical means to incorporate network and device security. These benefits directly lead to more accurate and secure MANET functional decisions as well as more efficient network operations.

There are two major contributions of this work. First, the ontological organization and structuring of MANET decision support data will make it easier to automate future decision algorithms. Secondly, the *MANET Distributed Functions Ontology* provides a much needed foundation for incorporating security factors as a means to enhance the decision processes of MANETs.

In Section 2, we give additional background information about MANETs and ontologies. Section 3 describes the structure of our ontology as well as provides a descriptive fragment of a typical entry. Section 4 lays out the operational vision reflecting the integration of the ontology into MANET operations. Section 5 provides a worked example based on a realistic MANET scenario that shows the powerful potential of an ontological approach to secure MANET management. Finally, Section 6 discusses related work and Section 7 summarizes our work to date and indicates possible directions for future work.

2. Background

In this section, we discuss the origins of Mobile Ad-hoc Network technology and explain the nature of the operational environment. We build a case for the inclusion of security factors into MANET operations. Additionally, we introduce some of the existing advancements in ontologies and define common terms intrinsic to ontological work.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
An Ontological Approach to Secure MANET Management	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School,Department of Computer Science,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Proc. of the Third International Conference on Availability, Security, and Reliability, (Barcelona, Spain), pp. 787-794, Mar. 2008

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**8**	

2.1 Mobile Ad-hoc Networks (MANETs)

Following the invention of the two-way radio and the advent of communication without stationary interconnecting wires, the next step was to organize "a set of mobile, radio-equipped nodes" into a communication network. Baker and Ephremides described an architecture based upon the varying connectivity and the changing topology of the High Frequency (HF) Intra-Task Force communication network. This network was required to adapt to the inherent mobility of Navy ships as they attempted to communicate at sea. This ground breaking work has transformed into what we presently call Mobile Ad-hoc Networks (MANETs) [2].

Generally, there are two types of ad-hoc networks: sensor networks and MANETs. Sensor networks are used to collect physical information about an object or area and relay that information back to a central collection point. MANETs, however, are deployed with the purpose of allowing *communication* between nodes on the move. Two factors drive MANET operations: decision making and optimization.

To compensate for the lack of a fixed infrastructure, devices in a MANET must cooperate in making decisions that enhance their ability to communicate. Networked devices must rely on their peers to pass messages and to gain services that the component devices require in the day-to-day operation of the MANET. Decisions made for the collective good of the network are made in areas such as network clustering (the grouping of nodes) [2, 3, 5], cluster-head selection [2, 3, 4], protocol selection [6, 7, 8], and security policy. MANET decision-making does not end with providing the network with its initial organization. The randomness of device movement and the unpredictability of the wireless medium make the network topology susceptible to rapid, unpredictable connectivity and topological changes. Device attributes may also vary widely as the devices use their already-constrained internal resources to conduct routing and other tasks required to keep the MANET functional.

The second factor driving MANET operations is optimization. In the ideal case, a decision made for the collective good of the MANET has to be efficient in order to best conserve the scarce resources that exist among the networked devices.

The quality and the optimality of every MANET decision relies on the quality of the underlying input parameters to the decision making process. The data are often hard to collect and combine within a coherent decision process due to the heterogeneity of the device and network characteristics.

Further hampering the quality of decisions is the fact that security factors are rarely incorporated, resulting in a decision that may be optimal for performance, but not optimal or even highly risky for secure communications. One notable exception to date has been the inclusion of the "trustworthiness" of a public key infrastructure (PKI) scheme-based certificate in MANET decision-making [4].

2.2 Ontologies

The term *ontology*, rooted in philosophy, describes the study of existence. Computer science (originally the artificial intelligence community) later adopted the term ontology to mean [9]:

1. "A theory of a modeled world"
2. "A component of knowledge systems"

Thus, besides the philosophical connotation of ontologies, there are pragmatic reasons for their use. Ontology, as an engineering tool, may be further defined by its use. The tool may provide the "representational machinery with which to instantiate domain models in knowledge bases," allow the querying of knowledge-based services, and represent the results from these queries [9].

The use of ontologies has become much more widespread since the World Wide Web Consortium (W3C) included the concept as an explicit layer in the standards stack for the futuristic *semantic web* [10]. The semantic web uses ontologies to specify standard conceptual vocabularies. This approach makes data exchange easier and knowledge databases more accessible throughout the World Wide Web. W3C is leveraging the ability of ontologies to normalize data into consistent terms and to provide inference from data due to linkages between common terms. The linkages are manifested as relationship rules among objects.

Within an ontological framework, *classes* are abstract groups, sets, or collections of objects. *Objects* are the basic individual items in the domain. *Attributes* are properties, or characteristics that objects can have and share. *Relations* are ways that objects may interact with each other. Ontologies are different from taxonomies, which do not incorporate the

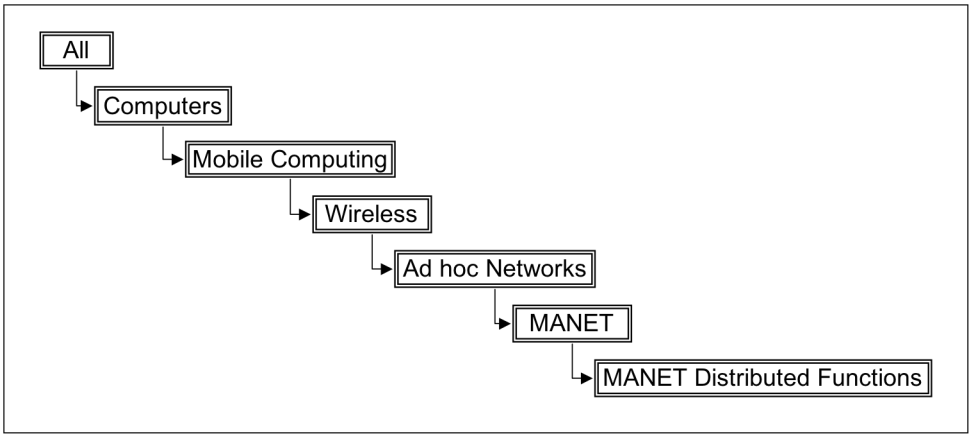

Figure 1. Conceptual organization of extended ontologies

▶ Content Portal	Acts as the focal point for the search , viewing, and download of content hosted on personal servers
▶ Cluster-head	Makes routing decisions on behalf of network
▶ User-specified Contact Node	The device where a specific user is logged into the system
▶ Lightweight Certificate Authority	(also called trust authority) manages the security certificates on behalf of the network
▶ MANET Rally Point	Serves as an assembly point if network communications irreparably break down
▶ Web Services Gateway	Provides web access to network devices that cannot connect
▶ Long-range Communications Service Provider	Provides capability to transmit messages over large distances
▶ Printer Service Provider	Provides printer access to network devices without one
▶ Photographic Service Provider	Provides the capability to take photos to nodes that are not camera-enabled or that require a photo of a specific item outside of their location
▶ Cross-domain Gateway	Serves as the link between MANETs at two different classification levels that wish to communicate
▶ Multilevel Secure Connection Node	Provides the maximum reachability to other MANETs of different security classification domains
▶ Policy Enforcement/Policy Decision Point	(e.g., for RADaC architectures) makes access control, authorization, authentication, and other security decisions related to the secure management of the MANET and its resources.

Figure 2. The *MANET Functions* Class

relations concept. A relation is an attribute whose value is another object in the ontology. Ontological relationships can specify arbitrarily complex rules about the attributes of the related objects, whereas a taxonomy has only the "is-a" relation. The set of relations taken as a whole fully describes the semantics of the domain.

Much of the research currently focused on ontologies is in the creation of top-level domain specific ontologies such as the Information Security Ontology [11] and the Stanford Wine Ontology, and the building of various general ontological databases. A challenge of this wide-spread research is to carefully define linkages between domain-specific ontologies to maintain the consistency of the root (all-encompassing) ontology.

3. MANET Distributed Functions Ontology

The domain of the MANET Distributed Functions Ontology (MDFO) is the functions or services that may be provided by component devices on behalf of other devices within a MANET. Before we describe the intricacies of the MDFO, we look at how our ontology potentially extends the root ontology provided by existing ontologies. An example conceptual organization of this extension is presented in Figure 1. This figure shows at an abstract level the potential linkages between our ontology and others that may occur. The top tier (root) of this hypothetical hierarchy is shown as the "All" ontology, which encompasses all of the ontologies in existence. The linkages reflected in the figure show either an "is-a" relationship or a meronymy "part-of" relationship. Thus, the MDFO is "part-of" the MANET ontology, which "is-an" object in the Ad hoc Network ontology, etc.

In the *MANET Distributed Functions Ontology*, there are three major classes. Each class comprises one or more objects; each object has one or more attributes; and each attribute may take the form of a complex data type with one or more values.

The *MANET Function* class (**Class I**) defines all distributed functions or services that a node in the MANET

- **Content Portal**
  - Name: content portal
  - Communication capability of node-pair link (intrinsic): {nil}
  - Communication capability of node-pair link (dynamic): {mobility rate, bandwidth of link, signal strength}
  - Device capability to support function (intrinsic): {user ID}
  - Device capability to support function (dynamic): {location, battery power, available memory}
  - Security of communications link: {authentication type, encryption algorithm and mode, compatibility of sensitivity levels, external assurance and functional evaluation level, resource hiding hardware}

Figure 3. Fragment of the *MANET Function* Class

- **Device 1499965**
  - Name: device 1499965
  - Communication capability of node-pair link (intrinsic) / connections: {longrange, wifi, bluetooth}
  - Communication capability of node-pair link (dynamic) / bandwidth of link: {11 Mbps}
  - Communication capability of node-pair link (dynamic) / mobility rate: {5 m/s}
  - Device capability to support function (intrinsic) / clock speed: {33 MHz}
  - Device capability to support function (dynamic) / available memory: {50 MB}
  - Security of communications link / authentication type: {biometric}

Figure 4. Fragment of the *Network Component Profile* Class

might need to perform on behalf of the network. The *Network Component Profile* class (**Class II**) is the class of all devices connected to the MANET and their attributes along with slotted values observed before and during network operation. The *Parameter* class (**Class III**) specifies attributes and their allowable values or ranges for the MANET Function and Network Component Profile classes. Thus, Class III defines the measurements and metrics pertinent to efficient MANET operations.

A list of the MANET Function objects (function names) and their definitions is shown in Figure 2.

If we open one of the objects within the *MANET Function* Class from Figure 2, the relationship between the functions and the parameters becomes quite clear (see Figure 3). For the Content Portal, certain attributes are intrinsic to the device, while others will change during operation and are dynamic. The "nil" value assigned to the "Communication capability of node-pair link (intrinsic)" indicates that there are no critical parameters for this category with respect to this particular function.

The *Network Component Profile* class contains all of the devices connected to the network as "objects" (Figure 4). Device 1499965 has the intrinsic and dynamic attributes given, with the measured values located within the braces. For every possible performance and security parameter, there is a separate attribute in the class.

The attribute value types in this ontology differ according to the anticipated input. In Figure 4, there are examples of a string type ({biometric}), a number type ({11}), and an enumerated type ({longrange,wifi, Bluetooth}).

As discussed earlier, the power of an ontology comes from the semantic links between its classes. The links allow for the ability to infer and interpolate among the objects in the ontology. In the next section (Section 4), we discuss the integration of the ontology into actual MANET operations.

4. Integrating the Ontology into an Operational MANET

The MANET Distributed Functions Ontology can serve as the basis for MANET decision making and optimization and correspondingly both control and facilitate the conduct of MANET operations. Our operational vision consists of a translator, the ontological database with function matching and inference capability, and the decision-making process (Figure 5). These components make up the MDFO Management Mechanism (MMM). The actual ontology, the MDFO, is an abstraction that guides the construction of the

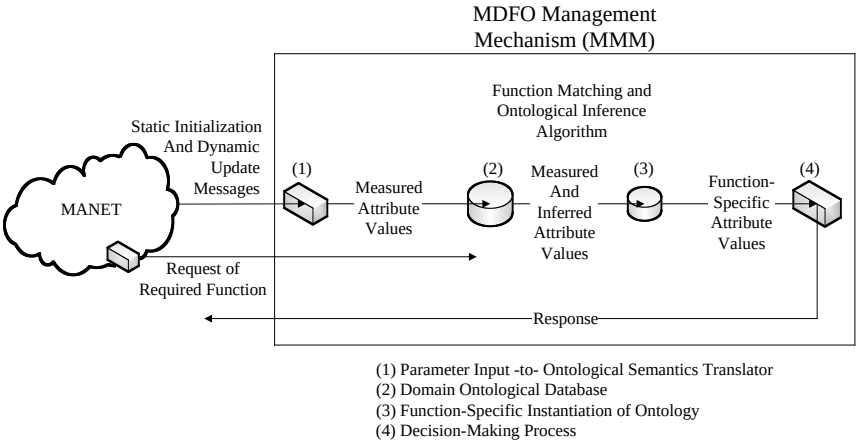

Figure 5. Operational vision

operational "ontological database."

The high-level operational vision can be explained as follows. For details, please refer to the worked example in Section 5. The translator is a mechanism for converting the information collected from the various messages circling the network, into the semantics of the ontology. The output of translation mechanism populates a database that is representative of the MDFO with both static and dynamic information about the devices within the MANET. The dynamic parameters will continue to be updated as MANET operations occur. When a function or service is required, a user or device may send a query to the MDFO. The ontology mechanism will instantiate (or take a subset of) the relevant portion of the ontology based on the service required, and an inference or interpolation may occur as needed. The inference may be required if parameters are not known or if the existing value is deemed to be outdated or unreasonable. The function-specific instantiation will then be available as input to a subsequent decision-making process.

To further explain the integration of the MDFO into MANET operations, it helps to look from the standpoint of the linkages between classes of the abstraction-level ontology. The three classes are shown below. The "categories" are the intrinsic, dynamic, and security attributes shown in Figures 3 and 4.

Class I: *MANET Function*
Objects: function names
Attributes: categories :
{**Values** = parameters (partial listing)}

Class II: *Network Component Profile*
Objects: device IDs
Attributes: categories / parameters (full listing) :
{**Values** = measured value}

Class III: *Parameter*
Objects: categories
Attributes: parameters :
{**Values** = value allowable range}

In the operation of the MANET (per Figure 5), the attributes in the ontology are assigned values. Classes I and III are pre-established to reflect the actual configuration of the MANET and its individual nodes, but expandable as needed. In Class II, the static (intrinsic) values of a portion of the attributes will also be pre-established. The dynamic values (measurements or metrics extracted from the MANET context and normalized in the translator) are entered into Class II during operations, per object (device ID) and attribute (categories / parameters). The dynamic values in Class II (measured values) are then checked against the values in Class III, where allowable attribute ranges are defined for accuracy.

When a function or service is required in the conduct of MANET operations, a user or a device inputs a request. Class I is referenced to find the set of parameters related to the desired function, and Class II is referenced to assign values for those parameters for each device ID involved in the request.

The logical flow of MANET operations is shown in Figure 6. The parallelograms represent input, the rectangles represent processing, the diamonds represent decisions, and circles are on-page continuations (i.e., a visual "go to"), here, from the left column of the figure to the right.

The next section provides a worked example to show hov

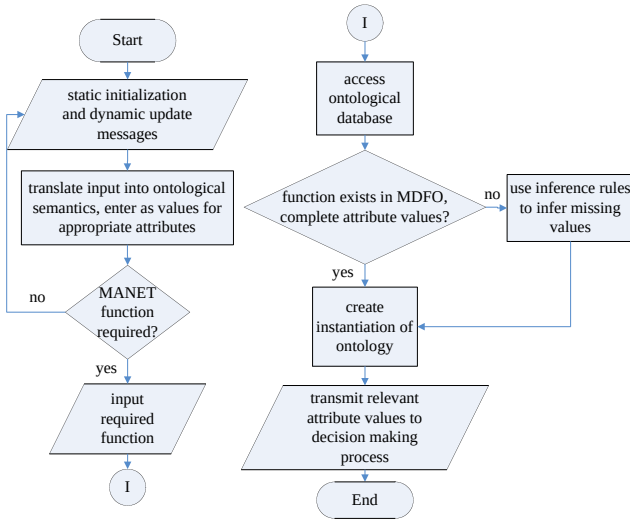

Figure 6. Flow chart of the operational vision

integrated into an operational MANET.

5. Worked Example

A realistic scenario involving five heterogeneous, MANET capable smart phones (see Figure 7) illustrates the operational vision described in Section 4 and demonstrates the value of integrating the *MANET Distributed Functions Ontology* into the context of a MANET implementation. The smart phones are the individual network components of the ontology. Each phone is shown to have a lightweight router, due to the requirement that every node must be able to participate in message passing. The axis is used to give a measure of the device locations.

A sampling of the smart phone characteristics appear in Table 1.

As is apparent, the MANET device information characteristics are disorganized and unwieldy. Additionally, the dynamic parameters listed above may change frequently during operation of the MANET.

5.1 MDFO Management Mechanism (MMM)

The MMM may reside in a dedicated node, or may be assigned as would be a "cluster-head," (e.g., to the node best suited for that responsibility in terms of processing, storage, and security characteristics), or it may be distributed. To guarantee the integrity of information, this mechanism may reside in a protected system such as a Mobile Trusted Module (MTM) [20].

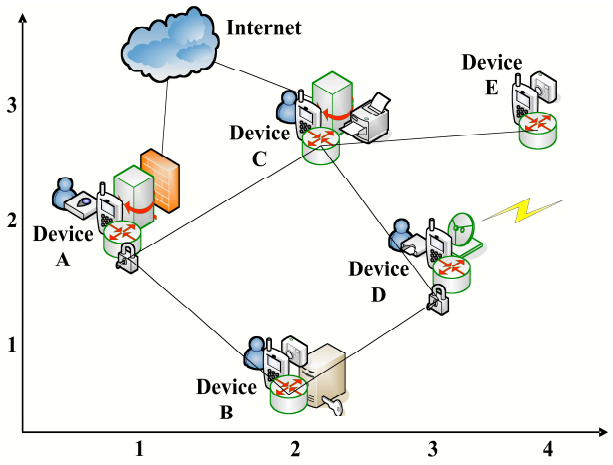

Figure 7. Worked example scenario

There are a few common ontological tools available to researchers, such as Stanford's Protégé [21], that show promise for holding data based upon the ontological model. Protégé allows users to build and populate ontologies. Additionally, the tool may be extended with a Java-based application programming interface to allow applications to access, use, and display ontologies. The current version of Protégé has yet to be extended to actual integrated network operations like the MDFO proposed in this paper. As a result of the lack of scalability of the ontological tools and resource limitations in the MANET nodes, and depending on the size of the MANET, a commercial lightweight database management system may need to be created to implement the MDFO Management Mechanism [22].

5.2 Initialization and Update of Static Attributes

Before any operations, the domain ontological database (shown in Figure 5) is initialized, filling an operational representation (e.g., the lightweight database management system) of Classes I and III and the static attributes of Class II. Static attributes for this worked example (Table 1) partially include clock speed, presence of resource hiding hardware, total memory, capabilities, user authentication, encryption, and the Common Criteria Evaluated Assurance Level (EAL) assigned to the device. The static attributes are not expected to vary as the MANET devices communicate.

The initialization of static (intrinsic) values occurs prior to the operational deployment of the MANET. Should a device be allowed to enter the MANET after initialization, that device transmits its static information to the MMM through a network management protocol (e.g., at the router level). For example, to represent the *external assurance and functional evaluation level*, a device may transmit a binary representation of the Common Criteria Evaluated Assurance Level (EAL) assigned to the device [12].

During operation, Class II dynamic attributes are collected, updating the device characteristics. Dynamic values can be collected by the MMM via passive listening, through polling of individual devices, or by receiving network

Table 1. Device characteristics

	Device A	Device B	Device C	Device D	Device E
Clock speed	620 MHz	620 MHz	33 MHz	620 MHz	33 MHz
Trust Zone	enabled				
TPM				enabled	
Total Memory	8 GB	8 GB	32 MB	6 GB	64 MB
Available Memory	4 GB	6 GB	20 MB	5 GB	50 MB
Power and battery (internet usage)	5.0 hours battery	6.5 hours battery	3.0 hours battery	9.0 hours battery	6.0 hours battery
Location	(1, 2)	(2,1)	unknown	(3, 2)	(4, 3)
Mobility rate	0.5 m/s	1 m/s	0 m/s	0 m/s	10 m/s
Controls		lightweight PKI server			
Activated Capability	Firewall	Camera			Camera
Inactive Capability			Printer	Long-range communications	
Bandwidth	AB (54 Mbps) AC (6 Mbps)	BA (54 Mbps) BD (40 Mbps)	CA (6 Mbps) CD (11 Mbps) CE (11 Mbps)	DB (40 Mbps) DC (11 Mbps)	EC (11 Mbps)
User Authentication	Biometric reader	Password	Password	Smart card reader	Password
Encryption	DES - CBC mode	Unknown	Unknown	DES - CBC mode	Unknown
Current session level	SECRET	SECRET	SECRET	SECRET	SECRET
EAL	5	4	3	5	5
User	System Administrator	High-level boss	Operator	Operator	Autonomous vehicle
Site	Secure operations center	Field	Open terminal (café)	Field	Field

management messages sent by devices that are new or have changed. The translator has to extract the parameter value and normalize it into terms consistent with the MDFO. The translator strips the layered header information from the obtained message and reads the data reflecting the input value. The translator will normalize the value into the correct form. In this worked example, if the MMM receives a message containing a device's Mobility Rate in miles per hour, it will convert the value to meters per second as required. Dynamic attributes from our worked example (Table 1) include the available memory, power and battery, and mobility rate.

5.3 Processing of Requests

When a distributed function is required during network operations, a user or a device sends a request to perform an operation to the MMM. For this worked example, we use the "content portal" described in the class fragment in Figure 3. A content portal is a MANET distributed function that aids in content management. This function is assigned to one of the nodes, which acts as the focal point for the search, viewing, and download of content that is hosted elsewhere on the MANET. An example distributed function request would be encapsulated with protocol-dependent information in the header and trailer:

```
<header> content portal <trailer>
```

The query for the content portal initiates the function matching and inference algorithm within the MMM. The request is matched to the respective object(s) in Class I of the ontology. The Class I object "content portal" contains information on which parameters are critical for this specific function. Each object (device) in Class II is then tailored to reflect the critical parameters. In this example, the Class II object "Device C" is modified. Note that because the clock speed is not as critical for a content portal as those parameters stated as attributes in Class I, it is not applicable (N/A) in the subset for this function. A fragment of the object "Device C" is below. The lead dots indicate that the full attribute name has been omitted.

```
Name = {device c}
…: mobility rate = {0} m/s
…: clock speed = {33} MHz     # N/A
…: location = {Unknown}
…: authentication type = {password}
```

The parameter values are evaluated for completeness and checked for accuracy against the value ranges in Class III. If there are missing or inaccurate values, they may be collected by the MMM as outlined in Section 5.2, or they may be inferred from the existing data when possible through the use of a set of inference rules. In our example, since location is an important parameter, Device C's location ("unknown") may be inferred. We know that the device has attribute "site" with a value "open terminal (café)". We could access a remote (not located within the MDFO) semantic ontology of cafés that have attributes of location, and *infer* the actual location of the device that way. An alternative is to *interpolate* the information based on the link directions to the neighboring devices of known location.

As an additional example of potential inference rules, certain security related parameters may be inferred. If we know the characteristics of the hardware (secure coprocessor, TPM enabled, etc.) or the external evaluation level, we can often infer that the overall security posture of the device is high, and, with reasonable confidence, assign the device high values for the remaining security parameters. Other non-MDFO ontologies may be tapped to assist with this inference action.

The output of the process is the function-specific attribute values. This output is the minimal set of values required to characterize a node's ability to perform the specific function (in this example, the content portal). Devices A through E would have a measured or inferred value for each of the attributes listed in Figure 3. A partial subset for "C" is below.

```
Name = {device c}
…: mobility rate = {0} m/s
…: location = {2,3}
…: authentication type = {password}
```

The minimal set of parameters for the devices in the MANET may then be fed into a decision-process and the device most capable of providing the content portal service may be selected.

6. Related Work

There have been many recent research advancements in both the introduction of security aspects into MANETs and the integration of ontologies into computer science.

Much of the security focus has been on securing routing protocols [13, 14, 15]. The approach used is typically limited to the application of cryptography certificates into a symmetric or lightweight PKI scheme. As a system for certificate management, work is ongoing on the use of Trust Authorities within the MANET [16]. The majority of the benefit functions that have been proposed for MANET decision-making center around metrics that reflect the "trust" of a node's performance, quantified as network events [3, 4]. However, security factors are rarely present in the decision-making.

Outside of the MANET-specific research, attempts to include security-related measurements and metrics into network decision-making have been made by adding an additional quality, "security," to the standard quality of service dimensions, called "QoP" or "QoSS." In this body of work, researchers attempt to create a "security-adaptable infrastructure" using "variant security." Security mechanisms and services may be varied, or tuned, within predetermined ranges to allow for a flexible security policy based on the network situation [17, 18].

Top-level ontologies are being created for every conceivable domain in order to start establishing common terminology and to facilitate natural language processing and artificial intelligence. One such example is an information security ontology [11]. The application of this proposed ontology was limited to creating a common language among

security researchers and the processing of natural language data sources. The integration of ontologies into actual network operations is rare. One of the few examples is in network management and control. Cleary et al. [19] applied ontological theory to configuration tasks in a network. In their system, Simple Network Management Protocol (SNMP)-based configuration messages are converted into ontological semantics, and a new network configuration plan is distributed to network nodes.

7. Conclusions and Future Work

Our work has enhanced the capability to understand the operational configuration of nodes in a MANET, allowing for a more accurate, security grounded decision-making process for dynamic MANET management. We have introduced the *MANET Distributed Functions Ontology*, which organizes the commonly used decision parameters and incorporates security parameters that are often neglected. We expect that the ontology's structural relationships, between the parameters and the dynamics of the MANET, may lead to reduced complexity in the decision making algorithm and improve the ability to make decisions in a more timely fashion. We expect the incorporation of security attributes and relations will enhance the ability to service the network as well as provide more robust security.

This work is a first step towards providing the optimized management of MANET functions and services. As an emerging technology, MANETs will gain in popularity as networks are deployed. The flexibility and the mobility of MANET technologies make them attractive to many organizations such as tactical military units, disaster response teams, and the ever-increasing social communications networks.

Future work includes the entry of the ontology into an automated tool in order to further investigate its potential for network management, to make the MDFO more accessible to other researchers, as well as to better assess the tool's potential to serve as an operational database in our integration of the ontology. Additionally, we plan to develop decision-making process functions that will take the minimal set of parameters as input and result in a near-optimal decision regarding which node is best suited to perform a particular function. Last, a study of whether the ontology and decision processing should occur in a centralized or a decentralized fashion within the MANET must be conducted.

References

[1] Donnelly, H., "Tactical Networker: Creating a Dynamic, Self-forming Network for Formations on the Move," *Military Information Technology*, vol. 10, is. 9, Oct. 2006.

[2] Baker, D.J., and Ephremides, A., "The Architectural Organization of a Mobile Radio Network via a Distributed Algorithm," *IEEE Transactions on Communications*, vol. COM-29, no. 11, Nov. 1981, pp. 1694-1701.

[3] Ghosh, R., Das, A., Som, P., Bhattacharya, R., Venkateswaran, P., Sanyal, S., and Nandi, R., "A Novel Optimized Clustering Scheme for Mobile Ad-Hoc Networks," *Proc. XXVIIIth URSI General Assembly in New Delhi*, Oct. 2005.

[4] Crosby, G., Pissinou, N., and Gadze, J., "A Framework for Trust-Based Cluster Head Election in Wireless Sensor Networks," *Proc. IEEE DSSNS*, 2006.

[5] Ho, C.K., Singh, Y.P., and Ewe, H. T., "An Ant Colony Optimization Approach to Building Clusters in Ad Hoc Networks," *Proc. of the Multimedia University International Symposium on Information and Communication Technologies*," Oct. 2004, pp. TS1B 1-4.

[6] Perkins, C., and Royer, E. "Ad hoc On-Demand Distance Vector Routing," *Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, Feb. 1999, pp. 90-100.

[7] Johnson, D., "Routing in Ad Hoc Networks of Mobile Hosts," *Proc. of the Workshop on Mobile Computing Systems and Applications*, Dec. 1994, pp. 158-163.

[8] Perkins, C., and Bhagwat, P., "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *Proc. SIGCOM 94*, Aug. 1994, pp. 234-244.

[9] Gruber, T., "Ontology," *Encyclopedia of Database Systems*, Springer-Verlag, 2008.

[10] Berners-Lee, T., Hendler, J., and Lassila, O., "The Semantic Web," *Scientific America*, May 2001, pp. 34-43.

[11] Raskin, V., and Nirenburg, S., "Ontology in Information Security: a Useful Theoretical Foundation and Methodological Tool," *Proc. of New Security Paradigms 2001*, Session 3, Sep. 2002, pp. 53-59.

[12] Karger, P., "A New Mandatory Security Policy Combining Secrecy and Integrity," *IBM Research Report*, RC21717 (97406), Mar. 2000.

[13] Adjih, C., Clausen, T., Jacquet, P., Laouiti, A., Muhlethaler, P., and Raffo, D., "Securing the OLSR protocol," *Med-Hoc-Net*, Jun. 2003.

[14] Winjum, E., Spilling, P. and Kure, O., "Trust Metric Routing to Regulate Routing Cooperation in Mobile Wireless Ad hoc Networks," *Proceedings of 2005 European Wireless (EW 2005)*, Apr. 2005, pp. 399–406.

[15] Sanzgiri, K., Levine, B., Shields, C., Dahill, B., and Belding-Royer, E., "A Secure Routing Protocol for Ad Hoc Networks," *Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02)*, 1092-1648/02, 2002.

[16] Reidt, S. and Wolthusen, S., "An Evaluation of Cluster Head TA Distribution Mechanisms in Tactical MANET Environments," *Proc. of International Technical Alliance in Network and Informational Science*, Sep. 2007.

[17] Irvine, C. and Levin, T., "Toward Quality of Security Service in a Resource Management System Benefit Function," *Proc. Of the Heterogeneous Computing Workshop*, Cancun, Mexico, May 2000.

[18] Levin, T., Irvine, C., and Spyropoulou, E., "Quality of Security Service: Adaptive Security," Handbook of Information Security, Volume 3, ed. H. Bidgoli, John Wiley and Sons, Hoboken, NJ, 2006, pp. 1016-1025.

[19] Cleary, D., Danev, B., and O'Donoghue, D., "Using Ontologies to Simplify Wireless Network Configuration," *Proc. Of Formal Ontologies Meet Industry Workshop*, Jun. 2005.

[20] Uusilehto, J., "Establishing Mobile Security," *TMC Internet Telephony*, vol. 10, no. 6, Jun. 2007.

[21] Protégé Home Page. (2007). [Online]. Available: http://protege.stanford.edu/

[22] Kaplan, A., "Applications for Real-Time Access", *Oracle Magazine*, May/Jun. 2006.